## REMARKS

In view of the following discussion, the Applicants submit that none of the claims now pending in the application is obvious under the provisions of 35 U.S.C. §103. Thus, the Applicants believe that all of these claims are in allowable form.

## I. REJECTION OF CLAIMS 1, 2, 7, 8, 13, 14, 20, 21, 24, 25, 28, AND 29 UNDER 35 U.S.C. § 103

Claims 1, 2, 7, 8, 13, 14, 20, 21, 24, 25, 28, and 29 stand rejected as being unpatentable over the Purtell et al. patent (U.S. 6,950,947, issued September 27, 2005, hereinafter "Purtell") in view of the Timm patent (U.S. 5,440,498, issued August 8, 1995, hereinafter "Timm"). The Applicants respectfully traverse the rejection. Specifically, the Applicants submit that Purtell and Timm fail to teach, show, or suggest several of the features recited in Applicants' independent claims 1, 7, 13, 20, 24, and 28.

Primarily, the Applicants submit that Purtell and Timm are completely devoid of any teaching, showing, or suggestion relating to the comparison of an alert (indicating an attack or anomalous incident) – or more specifically, the comparison of features of the alert - to the features of existing alert classes, in order to classify the alert, as claimed by the Applicants in independent claims 1, 7, 13, 20, 24, and 28.

The Examiner acknowledges in the Office Action that "Purtell does not [disclose] (b) identifying a set of potentially similar features shared by the new alert and one or more existing alert classes; (c) updating a minimum similarity requirement for one or more features; (d) updating a similarity expectation for one or more features; (e) comparing the new alert with one or more alert classes; and either: (f1) associating the new alert with the existing alert class that the new alert most closely matches; or (f2) defining a new alert class that is associated with the new alert" (Office Action, Page 3). The Examiner submits, however, that Timm teaches these missing features. The Applicants respectfully disagree.

By contrast, Timm teaches a method for evaluating and optimizing a security system for a physical facility (*e.g.*, "a building, manufacturing site or storage depot," Timm, column 1, lines 12-16). That is, the focus of Timm is on the elements of the security system (*e.g.*, "electronic sensors ... door and window switches," "reinforced

doors, walls and locks," and "guards or local authorities," Timm, Column 1, lines 19-26), and not on the alerts generated by the elements in response to an attack or anomalous incident. Although Timm teaches a method for comparing the effectiveness an element of the security system against the effectiveness of another element of the security system, again, Timm does not teach the comparison of alerts generated by the elements.

Since Timm does not teach the analysis of alerts that indicate an attack or anomalous incident, Timm cannot teach identifying a set of potentially similar features shared by the new alert and one or more existing alert classes; updating a minimum similarity requirement for one or more features; updating a similarity expectation for one or more features; comparing the new alert with one or more alert classes; associating the new alert with the existing alert class that the new alert most closely matches; or defining a new alert class that is associated with the new alert, as recited by the Applicants in independent claims 1, 7, 13, 20, 24, and 28. Thus, Timm fails to bridge the acknowledged gap in the teachings of Purtell.

Applicants' claims 1, 7, 13, 20, 24, and 28 positively recite:

1. In an intrusion detection system that includes a plurality of sensors that generate alerts when attacks or anomalous incidents are detected, a method for organizing the alerts into alert classes, both the alerts and the alert classes having a plurality of features, the method comprising the steps of:
(a) receiving a new alert;
(b) identifying a set of potentially similar features shared by the new alert and one or more existing alert classes;
(c) updating a minimum similarity requirement for one or more of the potentially similar features;
(d) updating a similarity expectation for one or more of the potentially similar features;
(e) comparing the new alert with the one or more existing alert classes; and either:
(f1) associating the new alert with a one of the one or more existing alert classes that the new alert most closely matches; or
(f2) defining a new alert class that is associated with the new alert. (Emphasis added)

7. A computer readable medium containing an executable program for organizing alerts that are generated by a plurality of sensors into alert classes, both the alerts and the alert classes having a plurality of features, where the program performs the steps of:
(a) receiving a new alert;

(b) identifying a set of potentially similar features shared by the new alert and one or more existing alert classes;

(c) updating a minimum similarity requirement for one or more of the potentially similar features;

(d) updating a similarity expectation for one or more of the potentially similar features;

(e) comparing the new alert with the one or more existing alert classes; and either:

(f1) associating the new alert with a one of the one or more existing alert classes that the new alert most closely matches; or

(f2) defining a new alert class that is associated with the new alert. (Emphasis added)

13. In an intrusion detection system that includes a plurality of sensors that generate alerts when attacks or anomalous incidents are detected, a system for organizing the alerts into alert classes, both the alerts and the alert classes having a plurality of features, where the system comprises:

(a) means for receiving a new alert;

(b) means for identifying a set of potentially similar features shared by the new alert and one or more existing alert classes;

(c) means for updating a minimum similarity requirement for one or more of the potentially similar features;

(d) means for updating a similarity expectation for one or more of the potentially similar features;

(e) means for comparing the new alert with the one or more existing alert classes; and

(f1) means for associating the new alert with a one of the one or more existing alert classes that the new alert most closely matches, or defining a new alert class that is associated with the new alert. (Emphasis added)

20. A method for organizing alerts into alert classes, both the alerts and the alert classes having a plurality of features, each of the plurality of features having one or more values, the method comprising the steps of:

(a) receiving a new alert;

(b) identifying a set of potentially similar features shared by the new alert and one or more existing alert classes;

(c) updating a similarity expectation for one or more feature values;

(d) comparing the new alert with the one or more existing alert classes; and either:

(e1) associating the new alert with a one of the one or more existing alert classes that the new alert most closely matches; or

(e2) defining a new alert class that is associated with the new alert. (Emphasis added)

24. A computer readable medium containing an executable program for organizing alerts into alert classes, both the alerts and the alert classes having a plurality of

features, each of the plurality of features having one or more values, where the program performs the steps of:

(a) receiving a new alert;

(b) identifying a set of potentially similar features shared by the new alert and one or more existing alert classes;

(c) updating a similarity expectation for one or more feature values;

(d) comparing the new alert with the one or more existing alert classes; and either:

(e1) associating the new alert with a one or the one or more existing alert classes that the new alert most closely matches; or

(e2) defining a new alert class that is associated with the new alert. (Emphasis added)

28. A system for organizing alerts into alert classes, both the alerts and the alert classes having a plurality of features, each of the plurality of features having one or more values, the system comprising:

(a) means for receiving a new alert;

(b) means for identifying a set of potentially similar features shared by the new alert and one or more existing alert classes;

(c) means for updating a similarity expectation for one or more feature values;

(d) means for comparing the new alert with the one or more existing alert classes; and

(e1) means for associating the new alert with a one of the one or more existing alert classes that the new alert most closely matches, or defining a new alert class that is associated with the new alert. (Emphasis added)

As discussed above, Purtell in view of Timm does not teach or even suggest the desirability of classifying of alerts that indicate an attack or anomalous incident by comparing features of the alerts to features of existing alert classes. Therefore, the Applicants submit that independent claims 1, 7, 13, 20, 24, and 28 fully satisfy the requirements of 35 U.S.C. §103 and are patentable thereunder.

Dependent claims 2, 8, 14, 21, 25 and 29 depend from claims 1, 7, 13, 20, 24, and 28 and recite additional features therefore. As such, and for at least the same reasons set forth above, the Applicants submit that claims 2, 8, 14, 21, 25 and 29 are not made obvious by the teachings of Purtell in view of Timm. Therefore, the Applicants submit that dependent claims 2, 8, 14, 21, 25 and 29 also fully satisfy the requirements of 35 U.S.C. §103 and are patentable thereunder.

## II. CLAIM AMENDMENTS

The Applicants have voluntarily amended the claims in order to correct minor

typographical errors.

## III. CONCLUSION

Thus, the Applicants submit that all of the presented claims fully satisfy the requirements of 35 U.S.C. §103. Consequently, the Applicants believe that all of these claims are presently in condition for allowance. Accordingly, both reconsideration of this application and its swift passage to issue are earnestly solicited.

If, however, the Examiner believes that there are any unresolved issues requiring the issuance of a final action in any of the claims now pending in the application, it is requested that the Examiner telephone Mr. Kin-Wah Tong, Esq. at (732) 530-9404 so that appropriate arrangements can be made for resolving such issues as expeditiously as possible.

Respectfully submitted,

5/15/08
Date

Kin-Wah Tong, Attorney
Reg. No. 39,400
(732) 530-9404

Patterson & Sheridan, LLP
595 Shrewsbury Avenue
Shrewsbury, New Jersey 07702